NETSCOUT

DDoS Threat Intelligence Report Issue 14

DDoS: The Next Generation

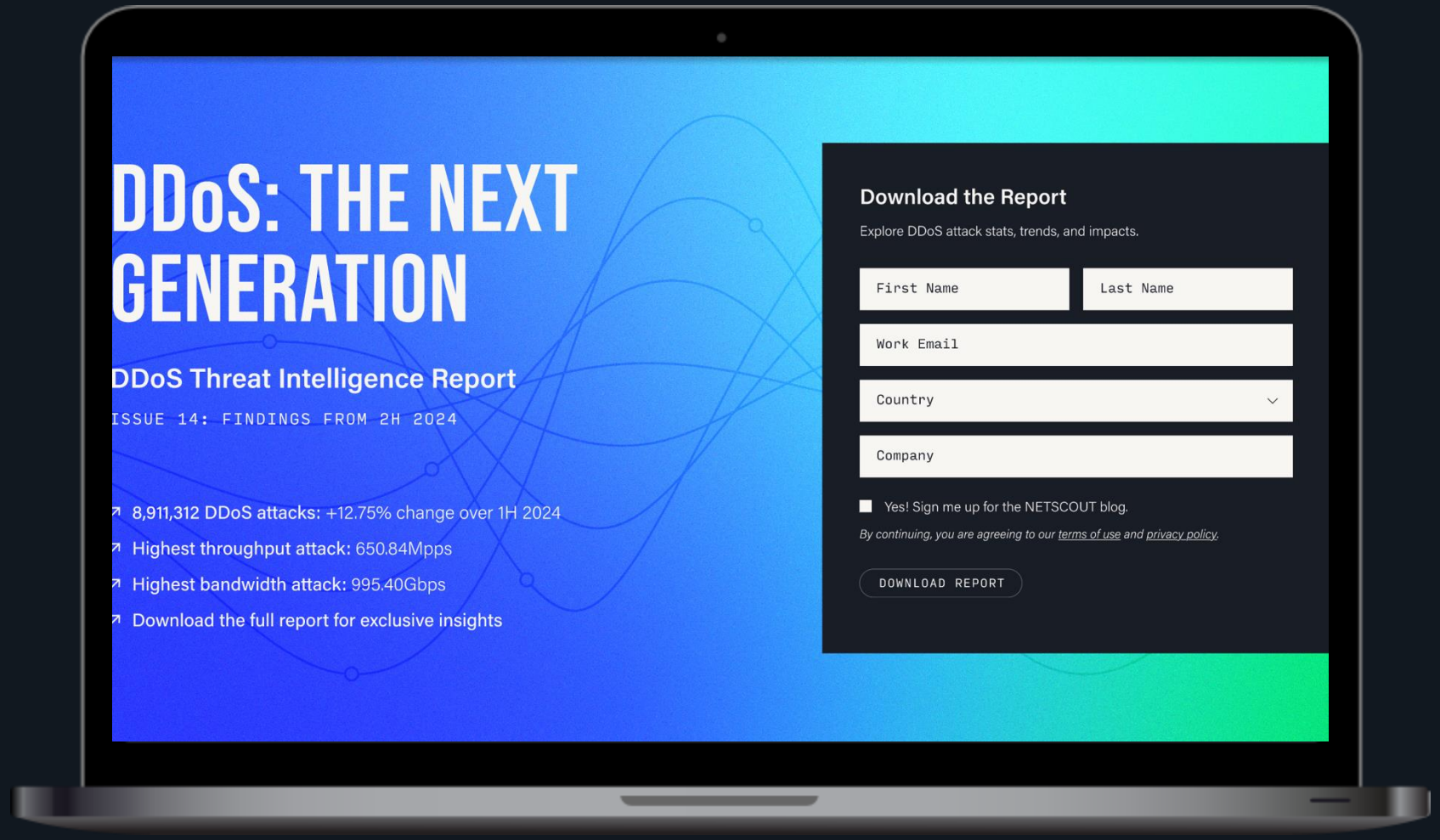
Andrew Cockburn, Chief Solutions Architect, NETSCOUT

COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

DDoS Threat Intelligence Report

Issue 14

www.netscout.com/threatreport



COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

NETSCOUT Intelligence – Global Attack Visibility

DDoS Data from 2/3 of routable IP space and ~1/2 of all internet traffic

700+ Tbps Most Tier-1 & 2 ISPs

500+ Service Providers

~2,000 Enterprise sites

125+ Countries

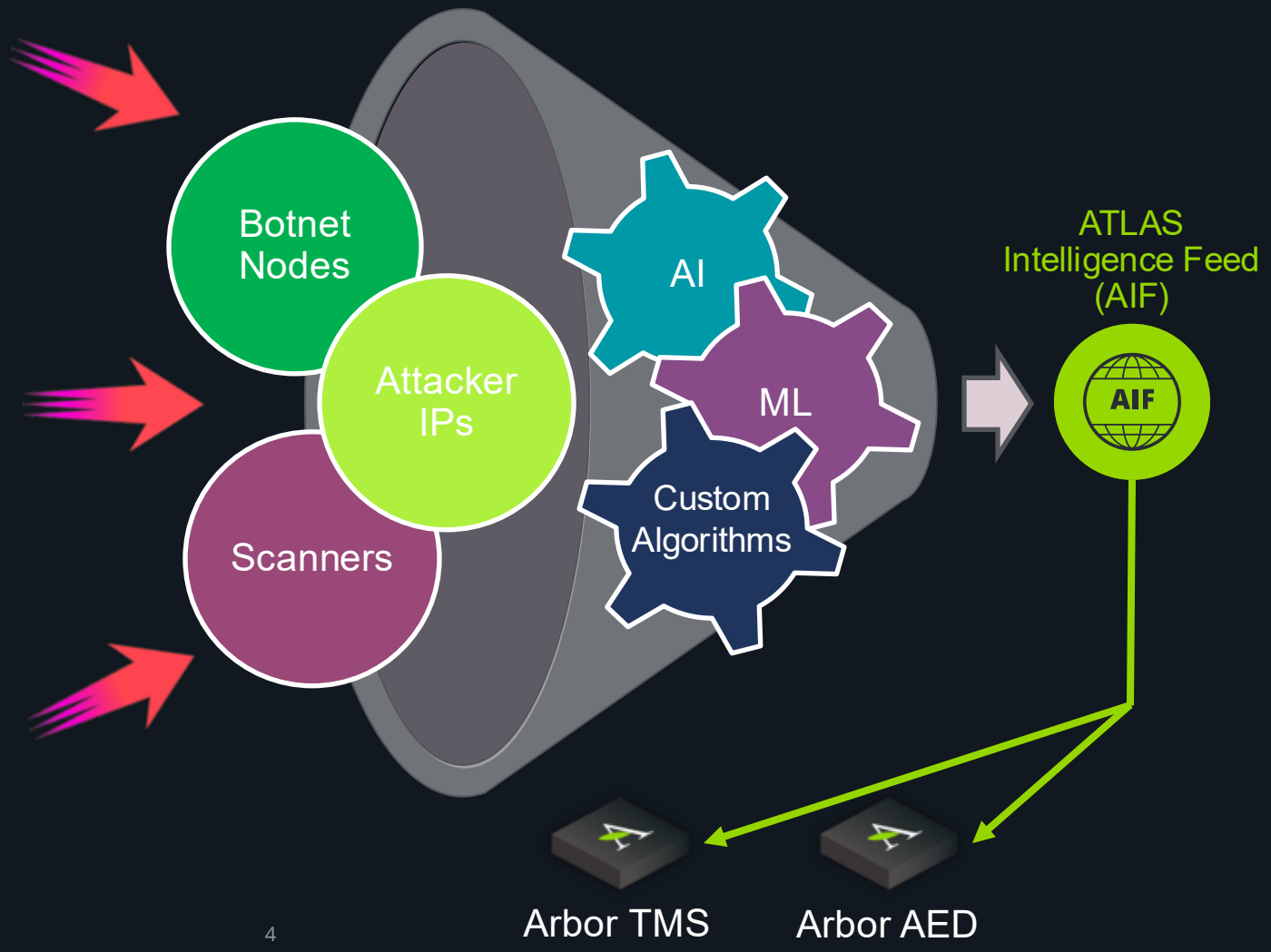


COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

AI/ML enabled Cloud Security Platform

Accurate And Actionable Intelligence from Massive Data Collection

- Cloud scale enables sophisticated AI/ML analysis with custom algorithms
- Massive unique global attack dataset
- Extracts the signal from the noise and eliminates false positives
- Outcome is highly accurate, actionable threat intelligence and DDoS insights



COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. |

Global Trends

COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

DDoS Attack Statistics

Max Bandwidth	995.40 Gbps
Max Throughput	650.84 Mpps
Attack Frequency	8,911,312* Attacks

* +12.75% change over 1H 2024

COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

Global Attack Stats

Bandwidth by Percentage	
<10Mbps	19.94%
10-100Mbs	19.32%
100Mbps-1Gbps	35.57%
1-10Gbps	20.81%
10-100Gbps	4.15%
>100Gbps	0.21%

Duration by Percentage	
<5 min	16.58%
5-15 min	53.78%
13-30 min	13.14%
30-60 min	6.57%
60+ min	9.93%

COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

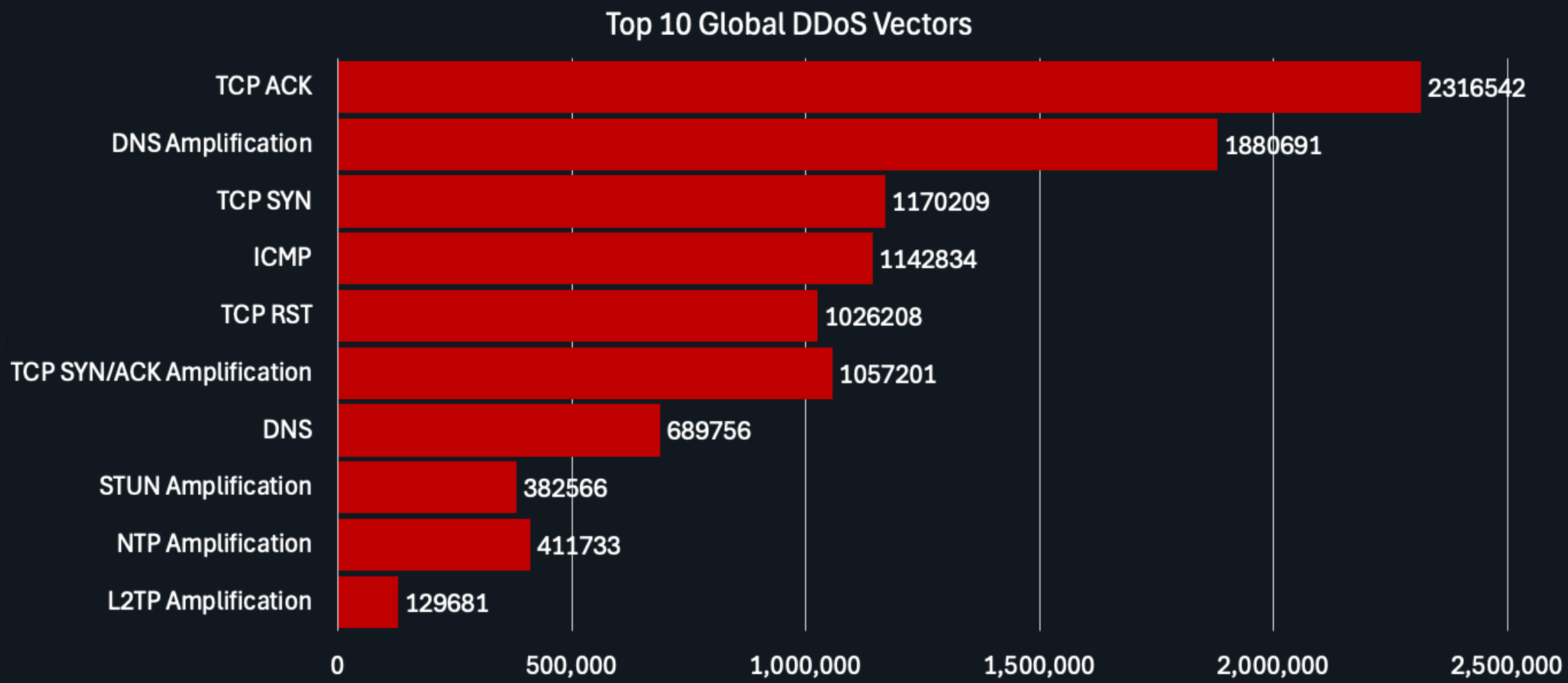
Global Attack Stats

Bandwidth by Percentage	
<10Mbps	19.94%
10-100Mbs	19.32%
100Mbps-1Gbps	35.57%
1-10Gbps	20.81%
10-100Gbps	4.15%
>100Gbps	0.21%

Duration by Percentage	
<5 min	16.58%
5-15 min	53.78%
13-30 min	13.14%
30-60 min	6.57%
60+ min	9.93%

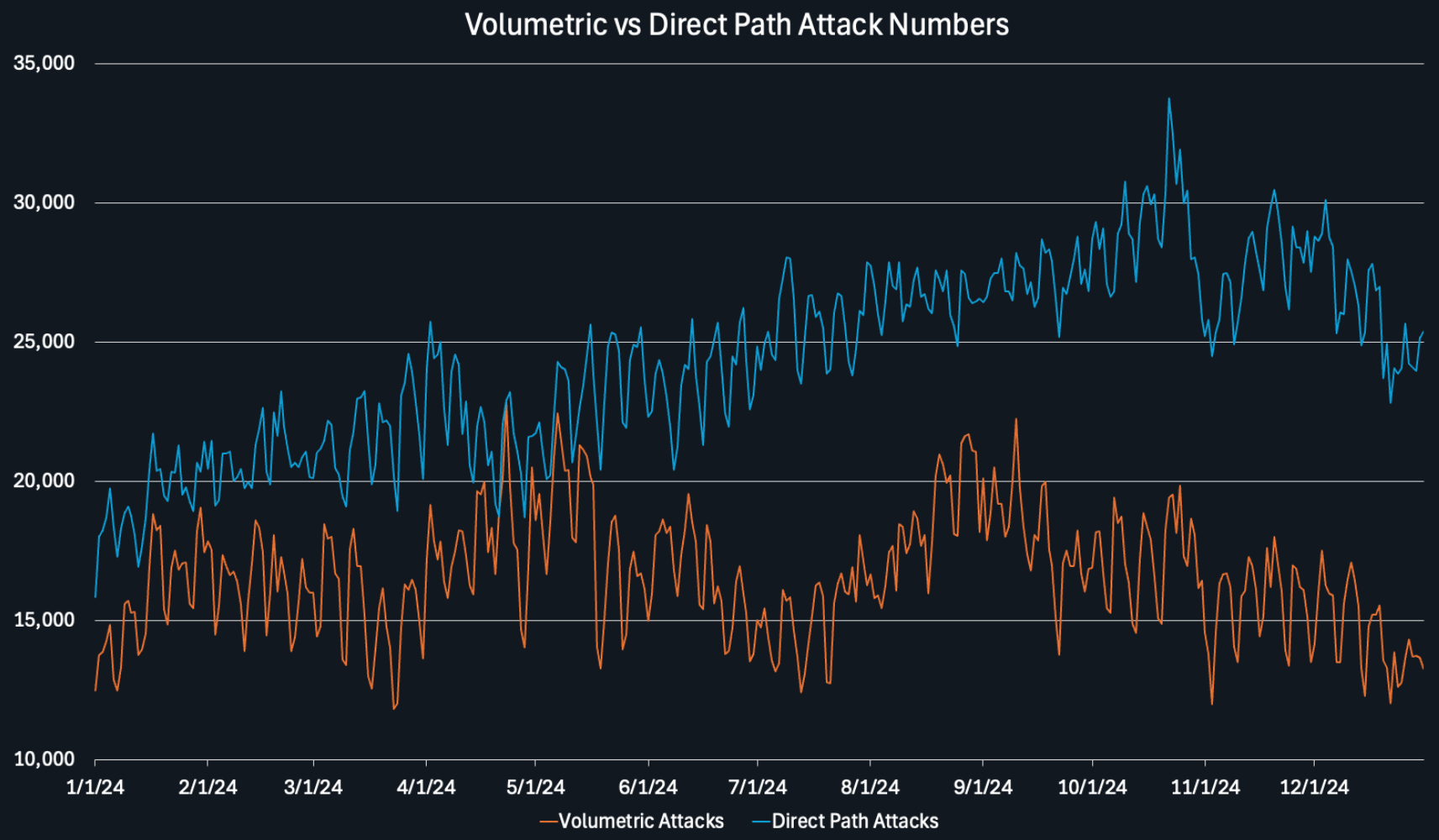
COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

Global Attack Stats



COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

Global Attack Stats



COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

Global & Regional Attacks

NAMER Highlights

Attack Count

1,585,495

+17.4% change over 1H 2024

LATAM Highlights

Attack Count

1,066,035

+29.83% change over 1H 2024

Global Highlights

Attack Count

8,911,312

+12.75% change over 1H 2024

EMEA Highlights

Attack Count

3,782,832

+5.2% change over 1H 2024

APAC Highlights

Attack Count

1,930,447

+19.62% change over 1H 2024

COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

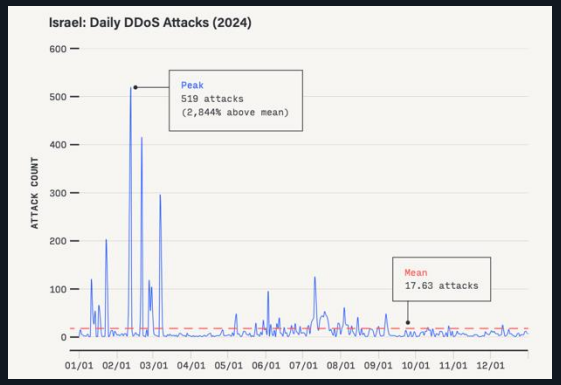
Geopolitical Motivations

COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

Geopolitical Motivations Drive DDoS Attacks



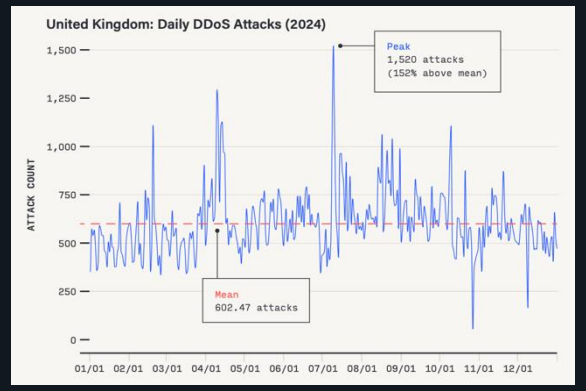
Israel



2,844% Increase aligned to Dark Storm Team's vow to attack, coinciding with Rafah operations



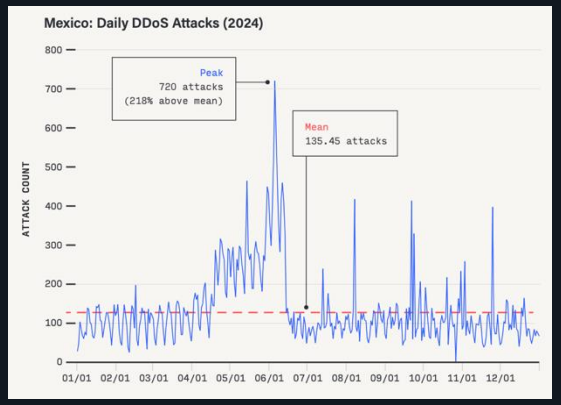
United Kingdom



152% Increase on the day Labor Party Parliament resumed session



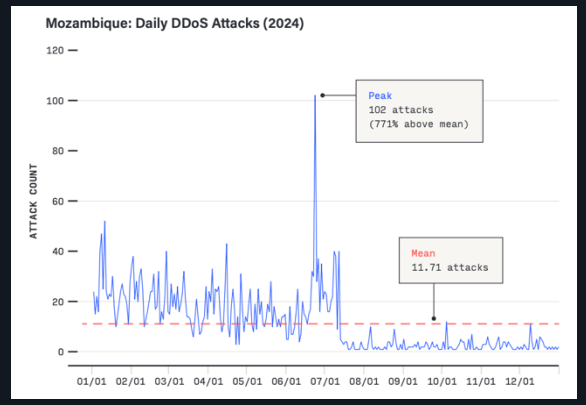
Mexico



218% Increase on the day of national elections



Mozambique

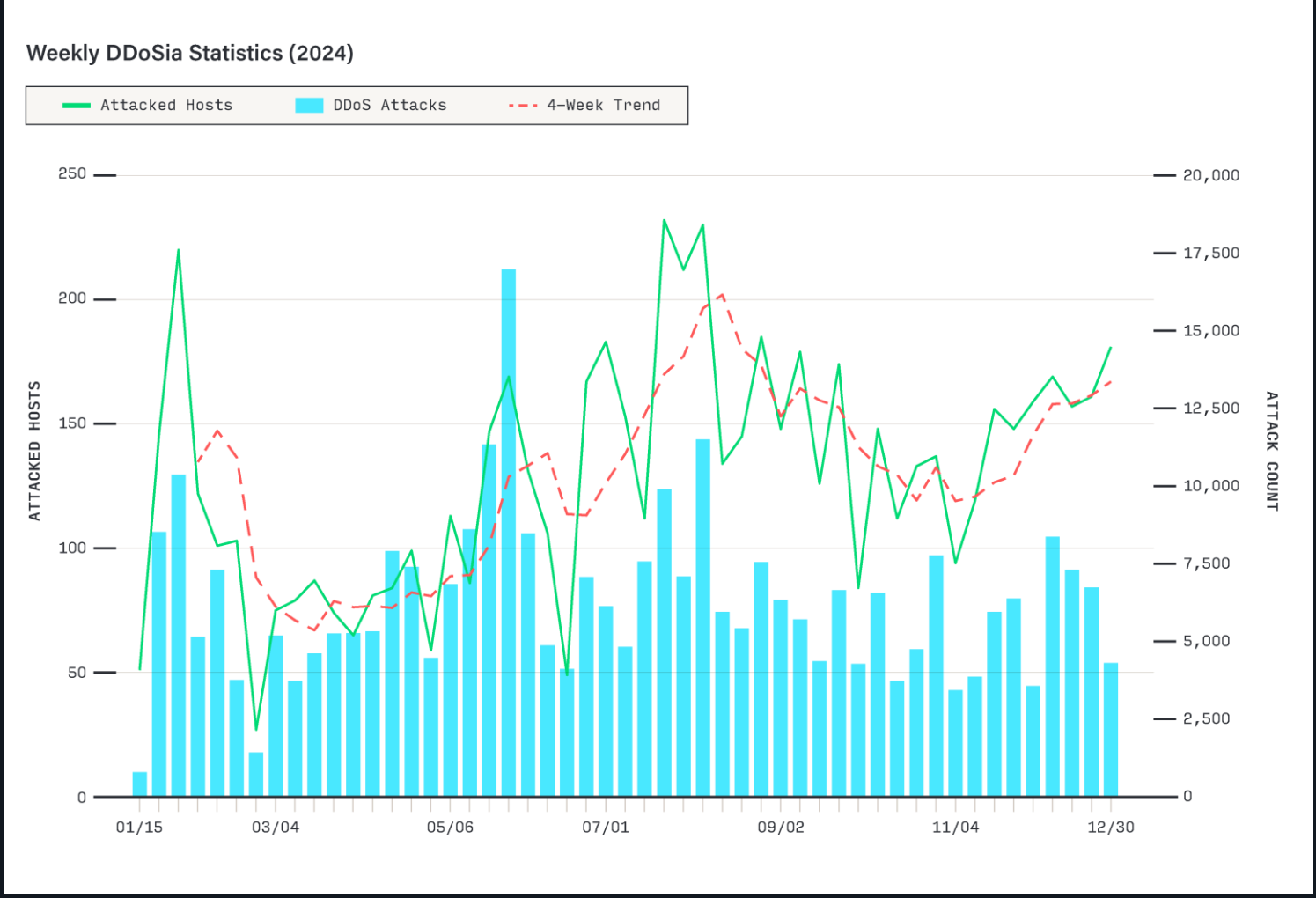


771% Increase around post-election protests

COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

NoName057(16) Still Most Prominent Hacktivist

Campaigns swarmed United Kingdom, Belgium, and Spain



COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

Next-Gen DDoS-for-Hire

COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

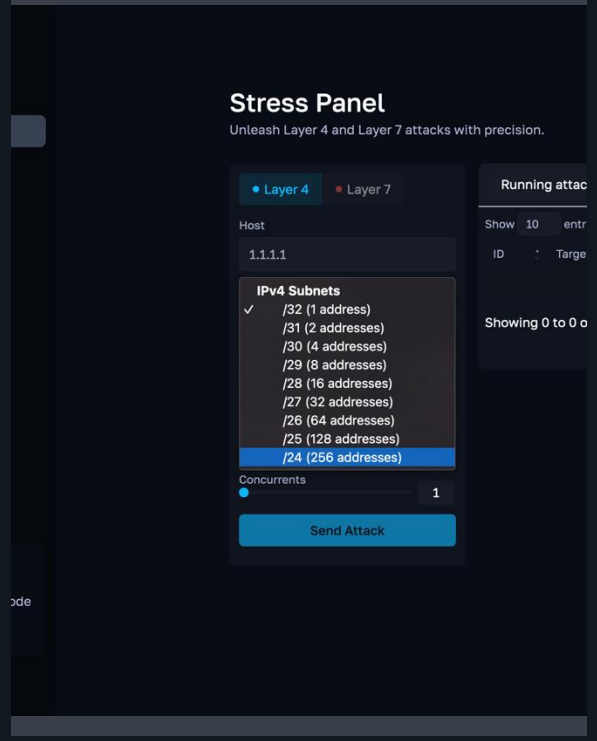
DDoS-For-Hire: Updates



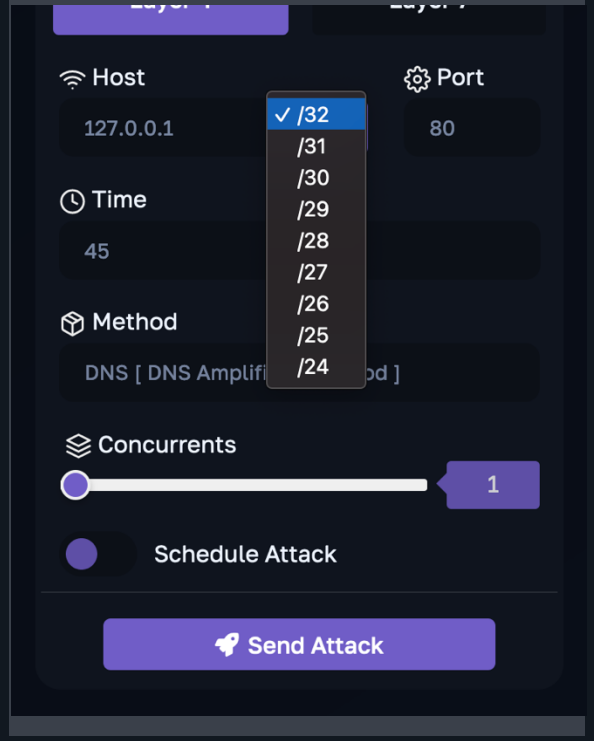
COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

DDoS-For-Hire: Carpet-Bombing

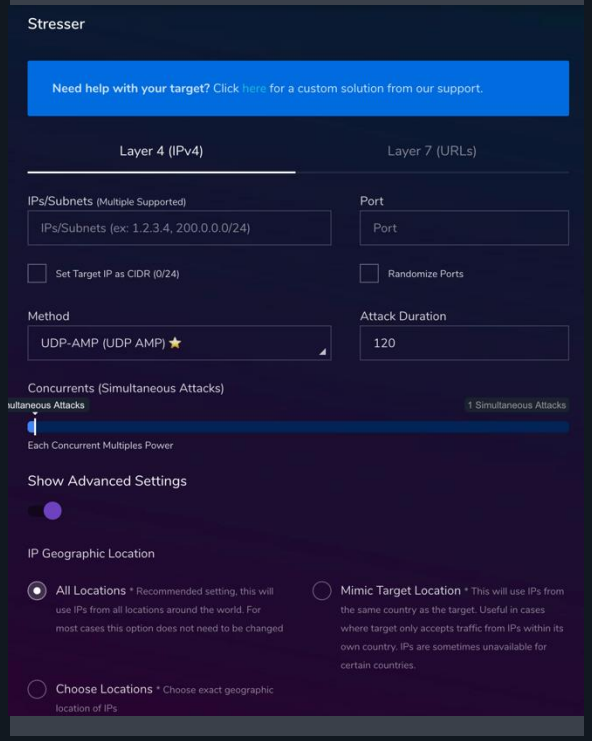
Up to /24



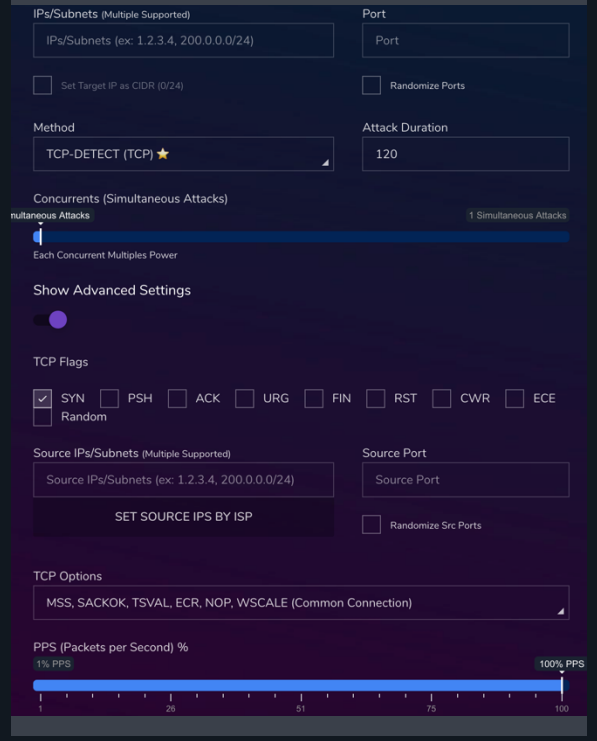
Up to /24



Range

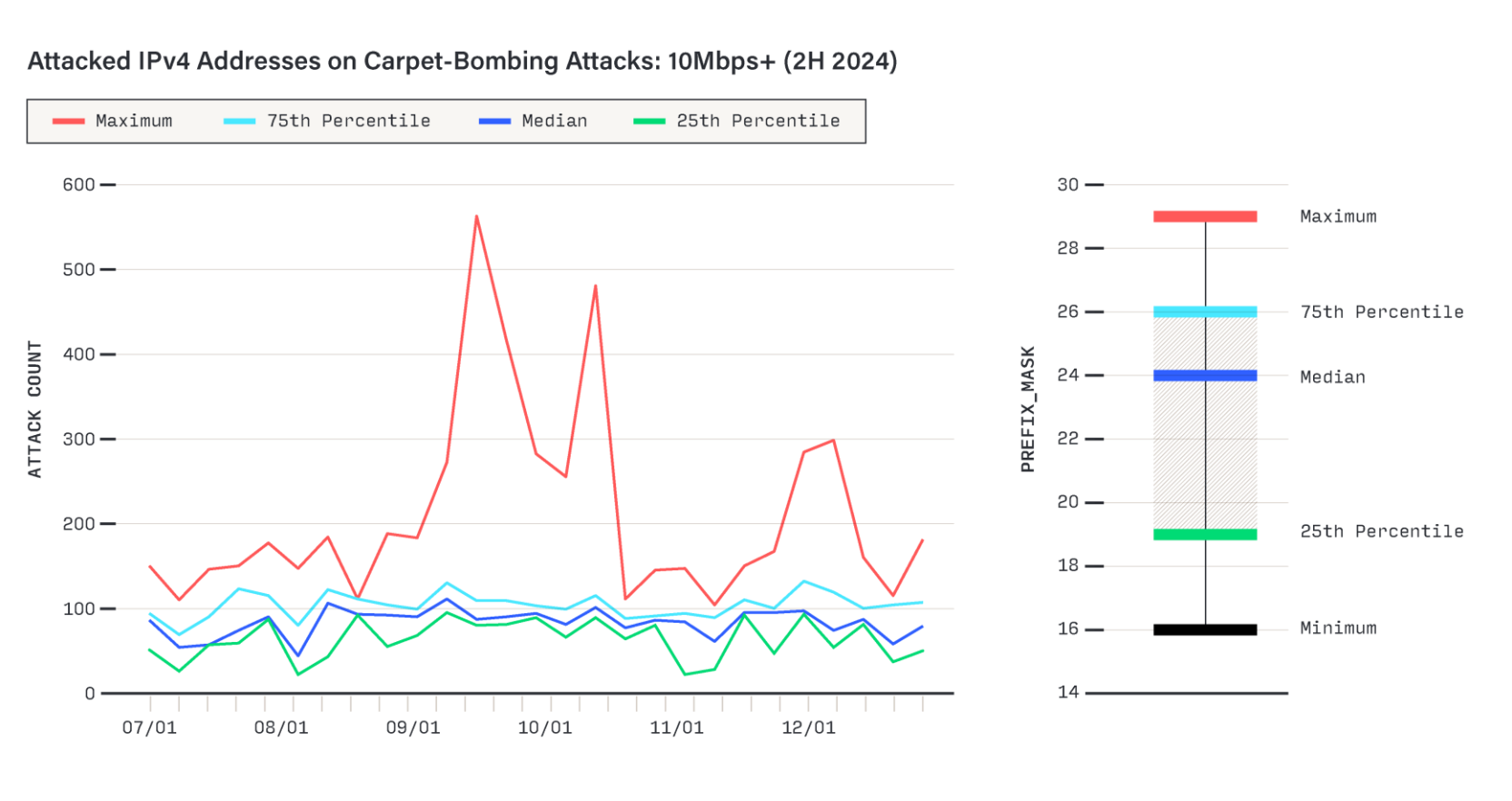


Range



COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

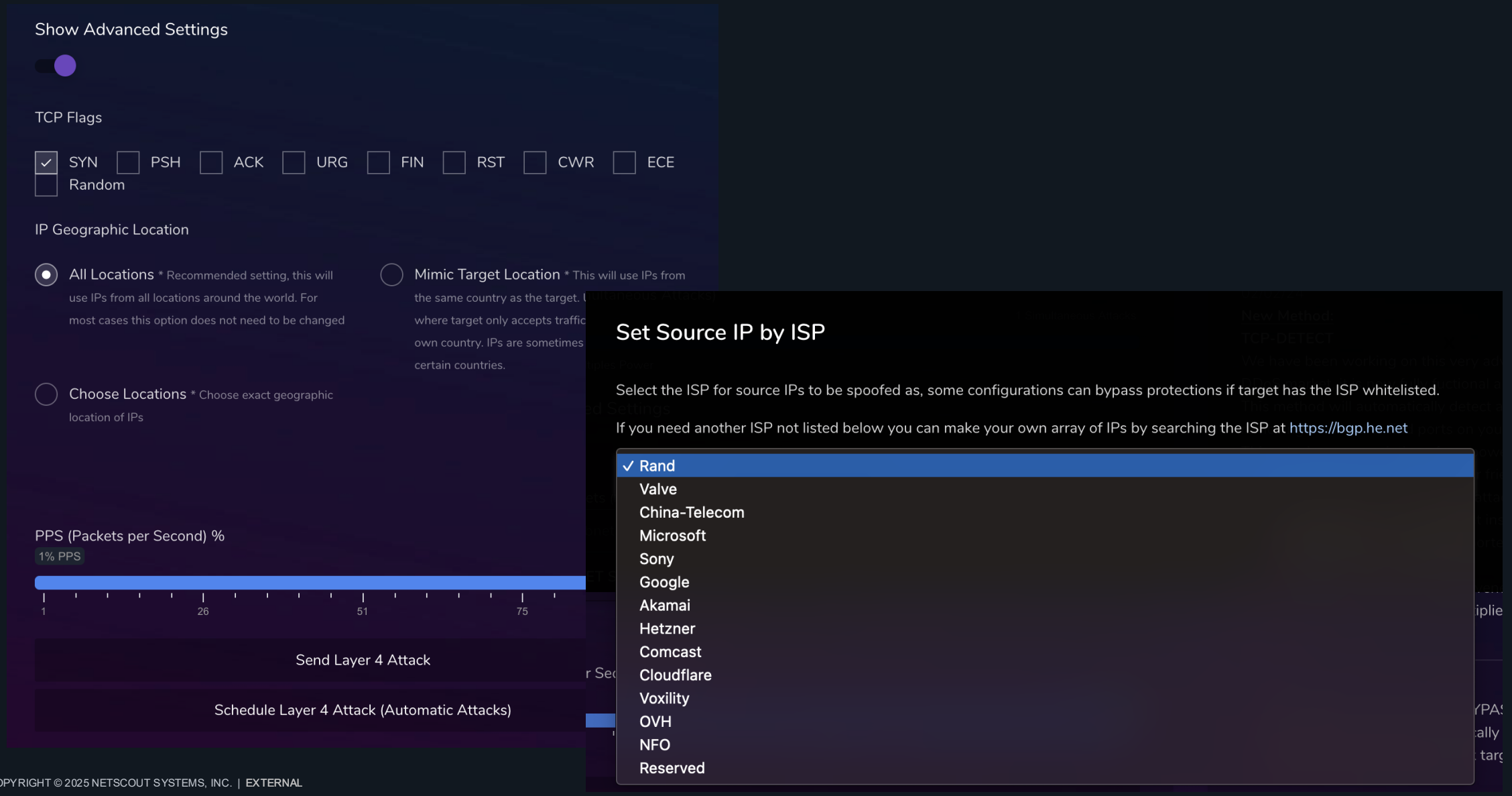
Carpet-Bombing: Global Statistics



Each attack targets an average of 100 IPs between a /20 and a /27 CIDR block

COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

DDoS-For-Hire: Geo/ISP Spoofing



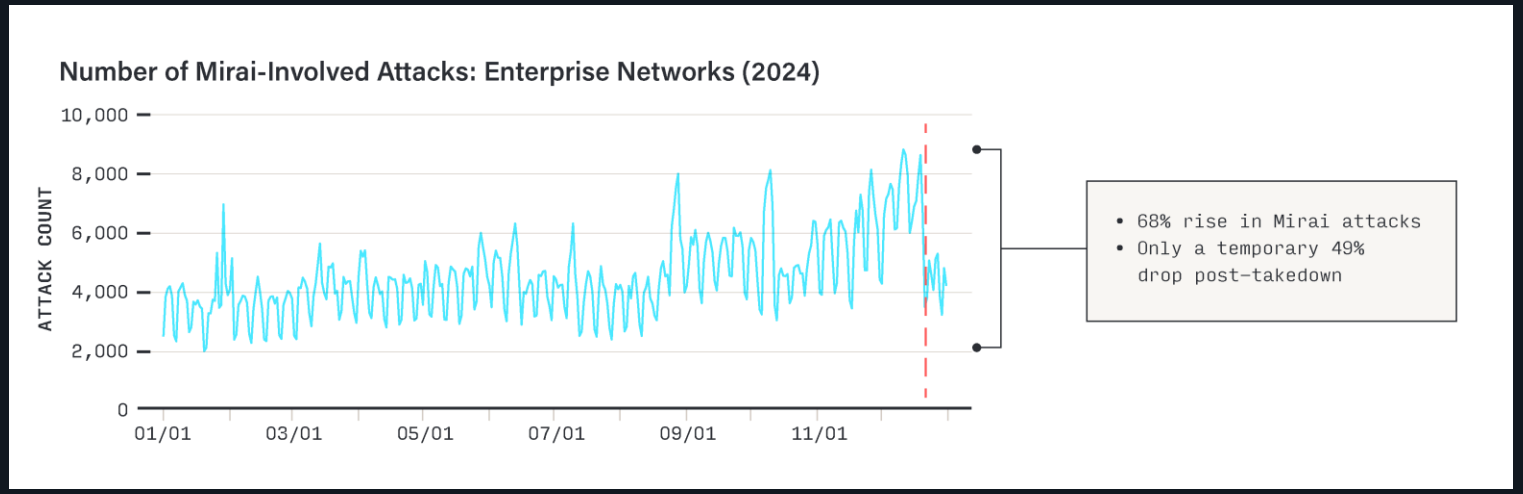
COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

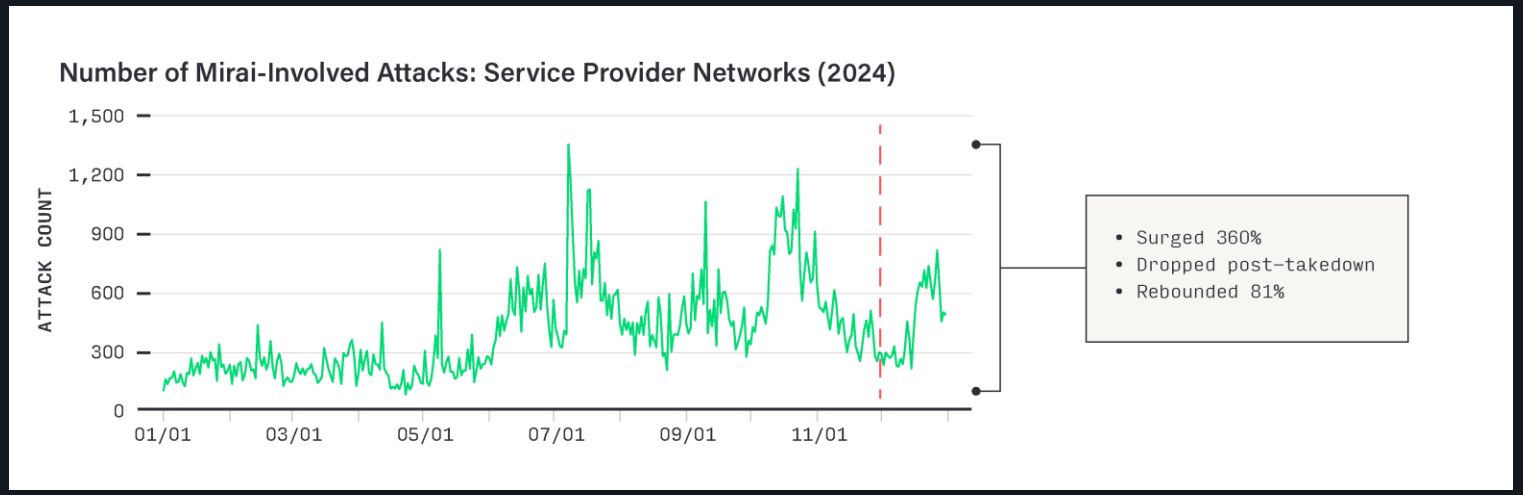
Botnets: The Backbone of DDoS-for-Hire Services

COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

Botnets: Increase Potency and Frequency of DDoS

- Meris nodes + 27%
- Dvinis nodes - 26%
- Mirai attacks on Service Providers + 360%
- Mirai attacks on Enterprises + 68%



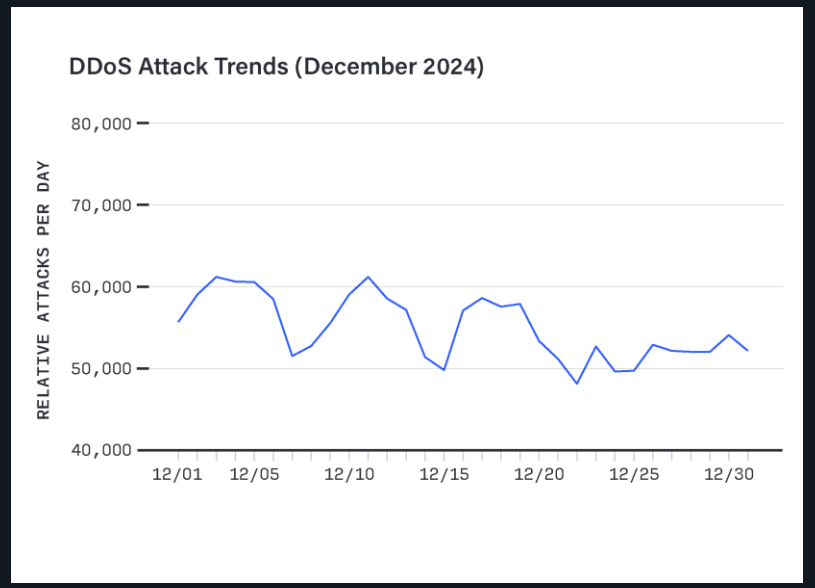


COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

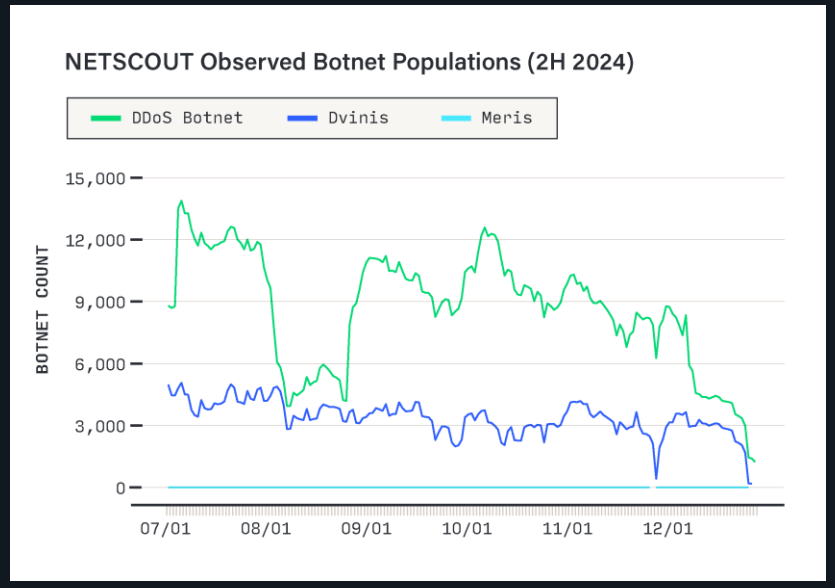
Botnets: DDoS-for-Hire Takedowns

Operation PowerOFF took down dozens of DDoS-for-Hire platforms in mid-December, a time when we typically see DDoS attacks plumet until the start of the new year.

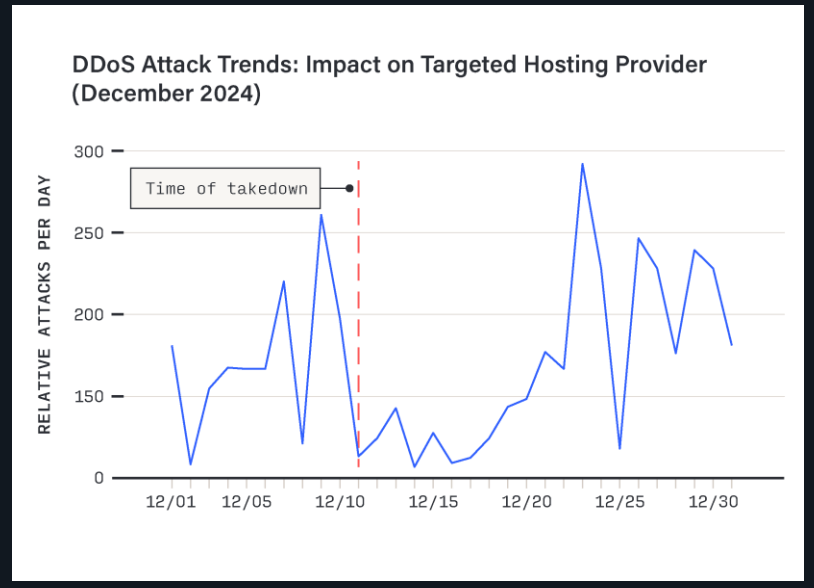
Botnet attacks adhered to yearly standards



Overall botnet population experienced multiple declines



Temporary attack reprieve, followed by resurgence



COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

Application Layer Attacks

Shifting Attack Trends

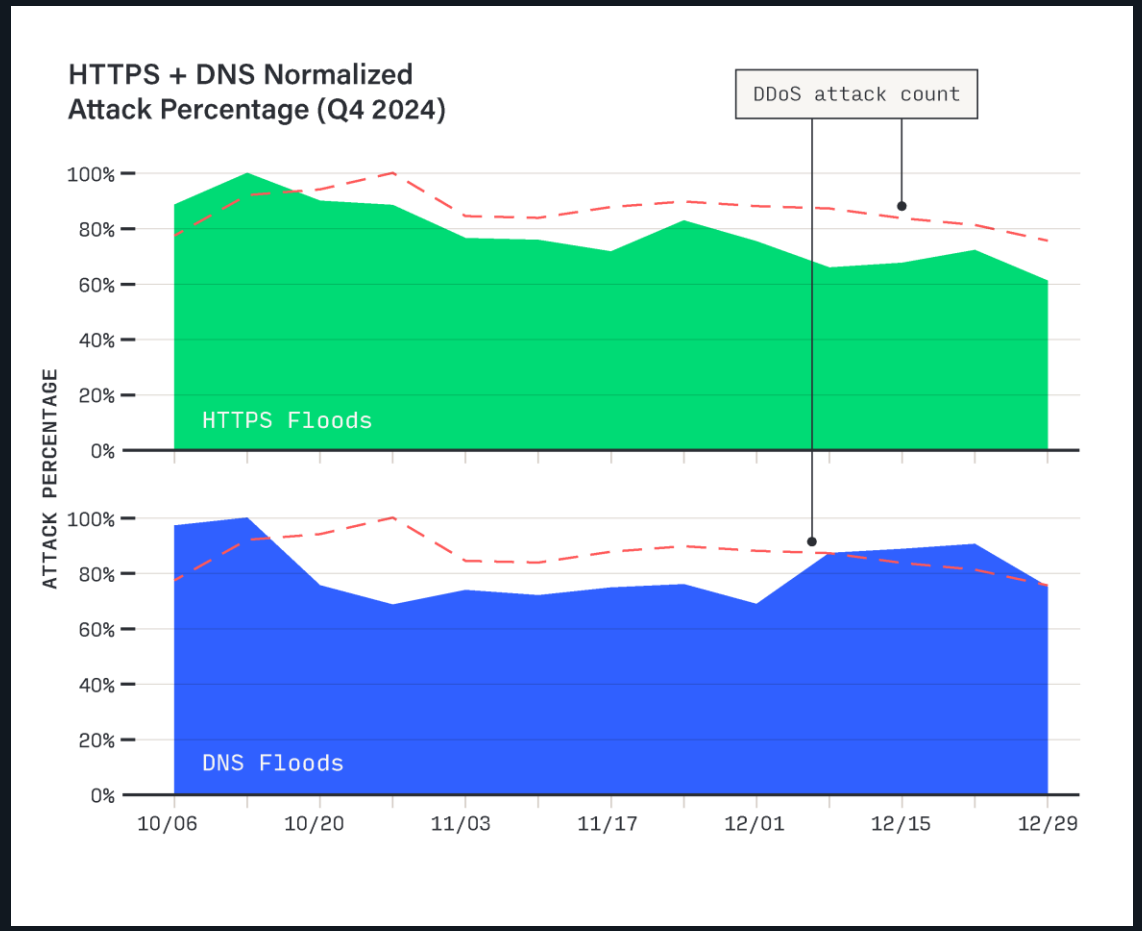
- DNS floods now surpass HTTPS in attack frequency showing a strategic shift

Proxy-Powered Attacks

- Proxies drive HTTPS and DNS flood attacks increasing complexity in detection and mitigation

Proxy Dependence

- Attackers rely heavily on cloud and residential proxies masking origins and evading defenses



COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

AI Takes the stage

COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

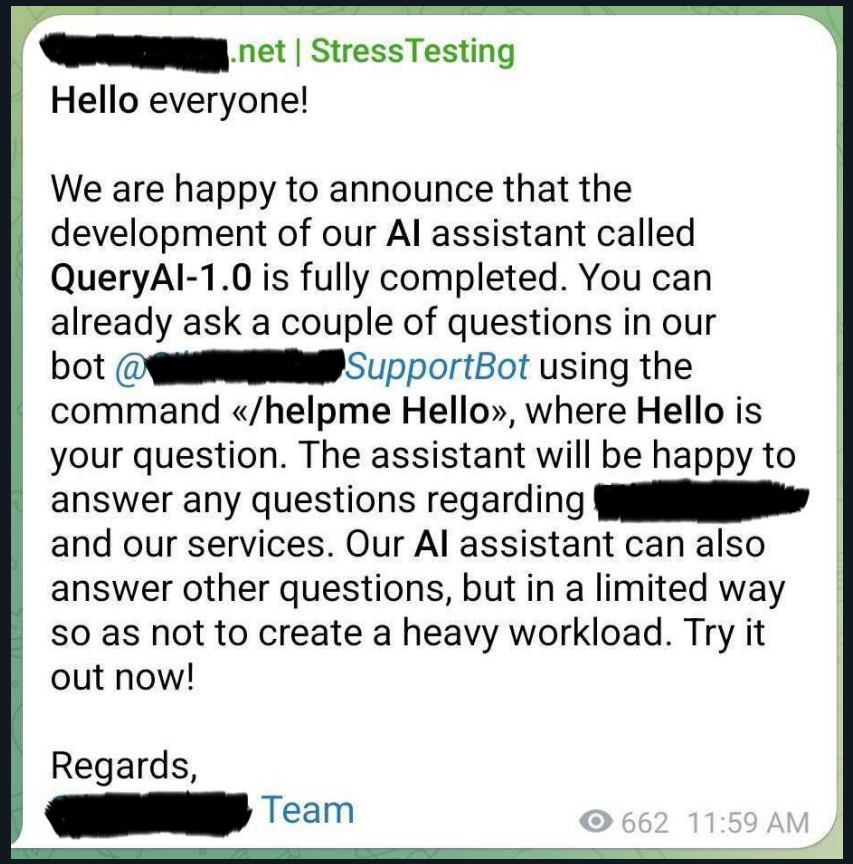
AI – What can we expect?

- The DDoS-for-hire ecosystem has already embraced automation extensively
- These platforms can now execute multivector attacks that adapt to defensive countermeasures, leverage IPv6 exploitation, and conduct carpet-bombing attacks across entire subnets.
- On the horizon, as AI is added to the mix:
  - AI-coordinated campaigns
  - AI-enhanced attacks that analyze defenses and work around them in real time
  - Conversational attack refinement

COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

AI – What can we expect?

- The DDoS-for-hire ecosystem has already embraced automation extensively
- These platforms can now execute multivector attacks that adapt to defensive countermeasures, leverage IPv6 exploitation, and conduct carpet-bombing attacks across entire subnets.
- On the horizon, as AI is added to the mix:
  - AI-coordinated campaigns
  - AI-enhanced attacks that analyze defenses and work around them in real time
  - Conversational attack refinement

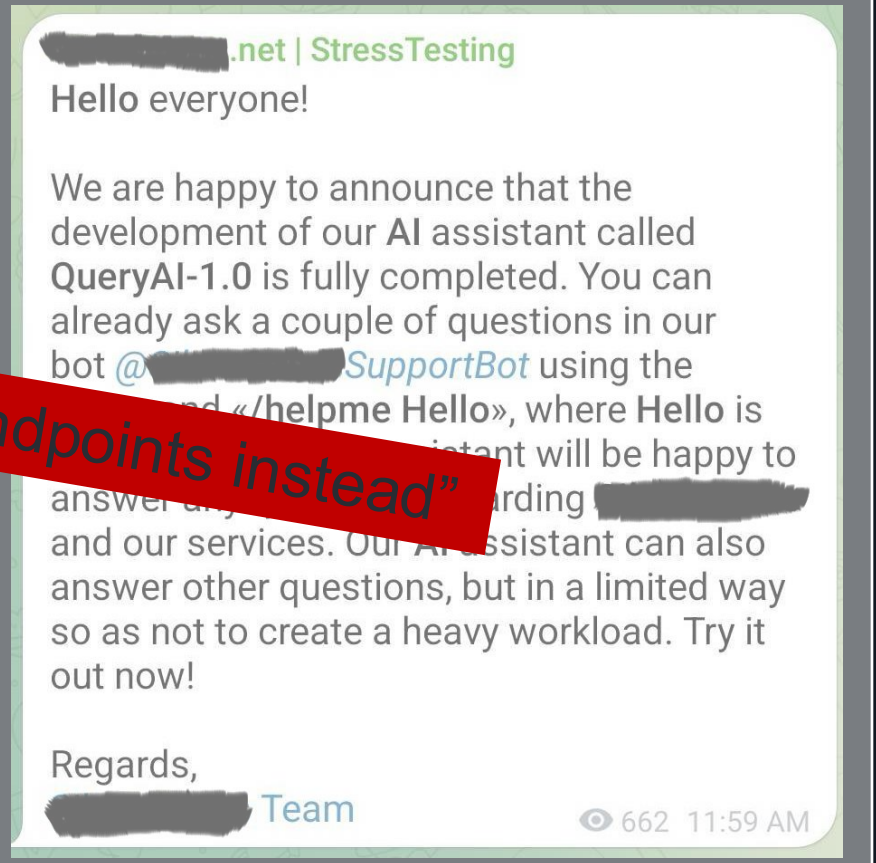


COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

AI – What can we expect?

- The DDoS-for-hire ecosystem has already embraced automation extensively
- These plat[redacted] can now execute multivector attacks that [redacted] countermeasures, leverage [redacted] and conduct carpet-bombing attacks across entire subnets.
- On the horizon, as AI is added to the mix:
  - AI-coordinated campaigns
  - AI-enhanced attacks that analyze defenses and work around them in real time
  - Conversational attack refinement

"That didn't work; try targeting their API endpoints instead"



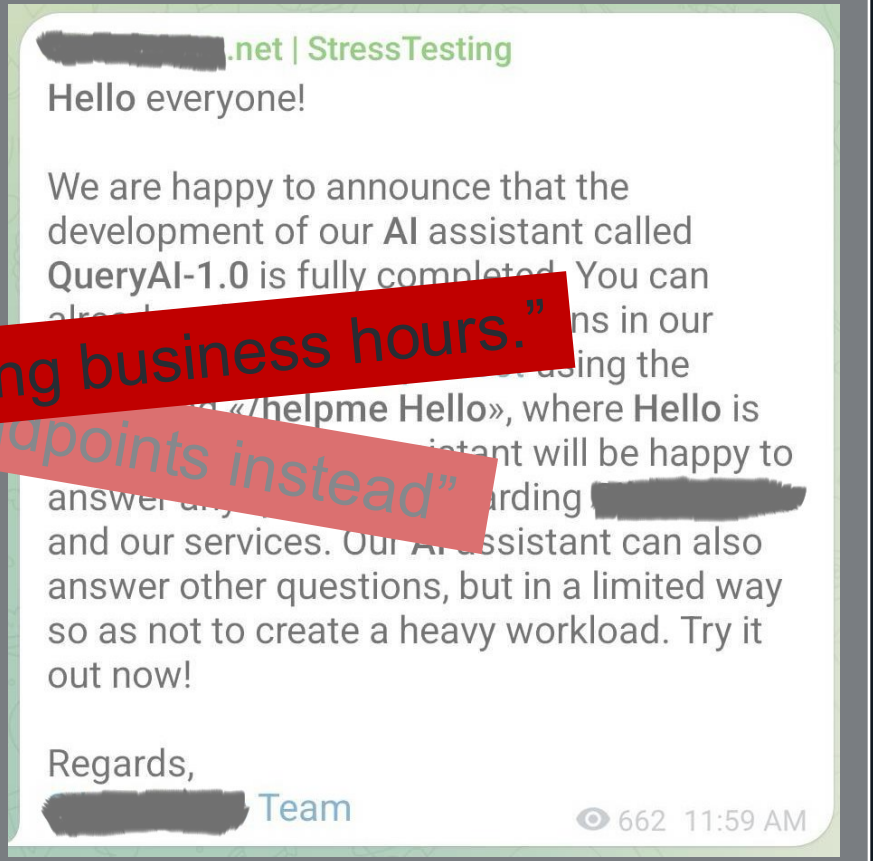
COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

AI – What can we expect?

- The DDoS-for-hire ecosystem has already embraced automation extensively
- These plat[illegible] can now execute multivector attacks that [illegible] countermeasures, leverage [illegible] and conduct carpet [illegible] entire sub[illegible]
- On the horizon, as AI is added to the mix:
  - AI-coordinated campaigns
  - AI-enhanced attacks that analyze defenses and work around them in real time
  - Conversational attack refinement

"That didn't work; try targeting [illegible] endpoints instead"

"Focus on their European data centers during business hours."



COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

How do we combat this?

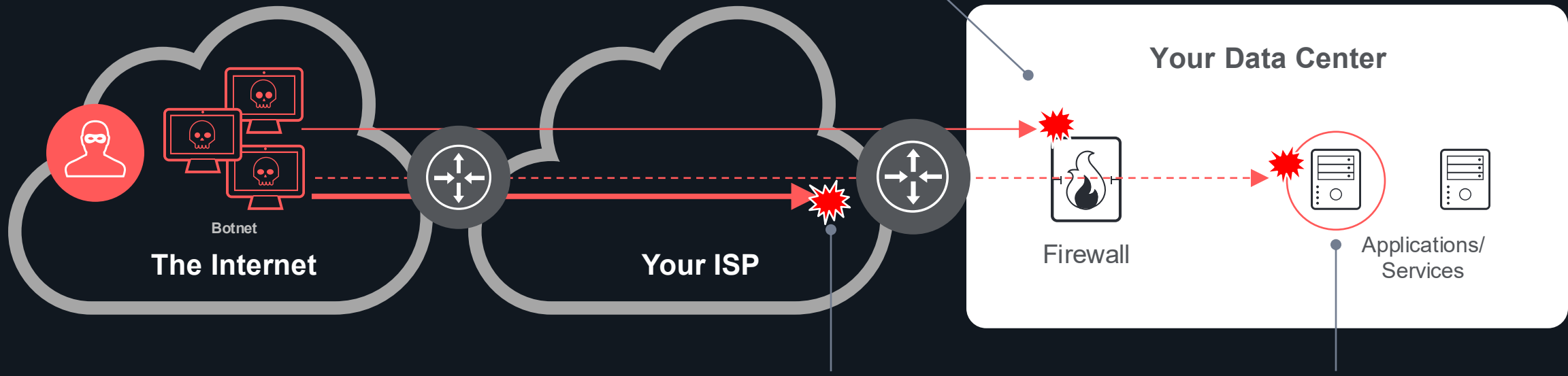
COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

Modern Day Attacks

Complex, Multi-Vector and Dynamic – Adaptive, Dangerous & Easy to Execute

TCP State-Exhaustion Attacks

- Crashes stateful devices (Load balancers, Firewalls, VPN Concentrators, IPSs)
- Critical during pandemic



Volumetric Attacks

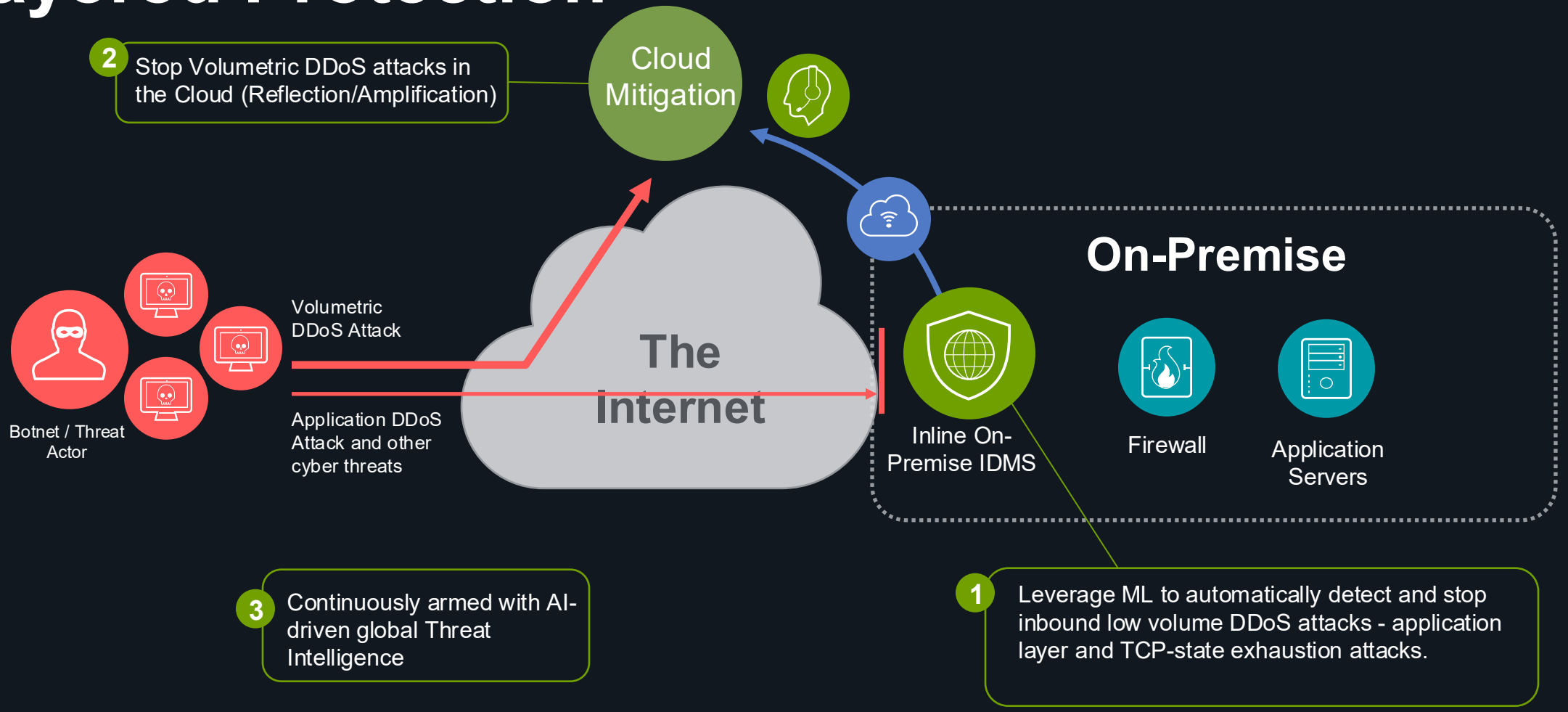
- Large(over Tbs)
- Saturates links

Application Layer Attacks

- Low and Slow, stealth attacks
- Crashes application servers

COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL CONFIDENTIAL

Stopping the Modern DDoS Attack Requires Layered Protection



COPYRIGHT © 2024 NETSCOUT SYSTEMS, INC.

DDoS Attacks can feel overwhelming …

- Good tools are important
- Preparation is key
- The most successful organizations prepare for this day
  - Best practice network hardening
  - Training
  - Simulations
  - Procedures
  - Up to date intelligence



COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

Want to experience this for yourself?

Learn how to attack AND defend at the DDoS Community!



COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL

NETSCOUT

THANK YOU

andrew.cockburn@netscout.com

netscout.com

COPYRIGHT © 2025 NETSCOUT SYSTEMS, INC. | EXTERNAL